

Verkkotunnusvälittäjän opas

Ohjeita ja vaatimuksia verkkotunnusvälittäjäksi
aikovalle

Versiohistoria

Versio	Päiväys	Kuvaus/muutos	Tekijä
1.0	25.10.2018	Versio 1	Ari-Matti Husa
1.1	21.12.2018	Versio 1.1	Ari-Matti Husa
1.2	6.9.2021	Päivityksiä KATAKRI-vaatimukseen (2.10.4)	Sami Salmensuu
1.3	15.12.2023	Päivityksiä välittäjän tietosuojavelvoitteisiin (2.7)	Mervi Malinen
1.4	19.1.2024	Päivitys rajoituksista EU/ETA-alueen ulkopuolisille välittäjille (2.7.1)	Mervi Malinen

Sisältö

1	Verkkotunnusvälittäjän tehtävät ja velvoitteet.....	5
1.1	Verkkotunnusvälittäjän palveluvelvoitteet.....	5
1.1.1	Rekisteröimisestä ja uusimisesta maksaminen.....	5
1.2	Velvollisuus neuvoa asiakkaita.....	6
1.2.1	Neuvonnan vähimmäisvaatimukset.....	6
1.3	Tietojen oikeellisuudesta ja ajantasaisuudesta huolehtiminen.....	7
1.3.1	Yhteystietojen päivittäminen.....	8
1.3.2	Lakisääteinen prosessiosoite ja muut sähköpostiosoitteet.....	8
1.4	Verkkotunnuksen uusiminen.....	9
1.4.1	Välittäjän velvollisuudet verkkotunnuksen voimassaoloajan päättyessä.....	9
1.5	Verkkotunnuksen irtisanominen.....	9
1.5.1	Irtisanomisen ongelmatilanteet.....	10
1.6	Verkkotunnuksen siirtäminen uudelle käyttäjälle.....	10
1.6.1	Oikeus tehdä verkkotunnuksen siirtopyyntö.....	10
1.6.2	Verkkotunnuksen siirtoaika.....	11
1.7	Välittäjän vaihtaminen.....	11
1.7.1	Välittäjän vaihtoavain.....	12
1.7.2	Verkkotunnus ilman välittäjää.....	12
1.7.3	Ongelmatilanteet.....	12
1.8	Välitystoiminnan päättyessä.....	12
1.8.1	Liikenne- ja viestintäviraston kieltopäätöksestä ilmoittaminen.....	13
1.8.2	Ennakkomaksutilin sulkeminen.....	13
2	Välitystoiminnan tietoturva.....	13
2.1	Tietoturva käytännössä.....	14
2.1.1	Tietoturvan osa-alueet.....	15
2.2	Riskien hallinta.....	16
2.3	Tietoaineistot.....	18
2.3.1	Aineistojen luokittelu ja käsittely.....	18
2.3.2	Tietoaineistodokumentit.....	18
2.4	Tietoturvan valvonta.....	19
2.4.1	Uhkien havainnointi.....	19
2.4.2	Uhkien ennaltaehkäisy.....	19
2.4.3	Valvonnan dokumentointi.....	20
2.5	Uhka- ja häiriötilanteiden hallinta.....	20
2.5.1	Menettelyohjeiden merkitys.....	20
2.6	Muutosten hallinta.....	21
2.6.1	Muutostöiden suunnittelu.....	21
2.6.2	Muutostöiden dokumentointi.....	21

2.7	Välitystoiminnan tietosuojaja	22
2.7.1	Fi-verkkotunnusvälittäjä henkilötietojen rekisterinpitäjänä.....	22
2.7.2	Fi-verkkotunnusrekisteriin ilmoitettavat henkilötiedot ja välitystoiminnassa käsiteltävät henkilötiedot	24
2.7.3	Henkilötietojen käsittelyn tarkoitus ja kesto	24
2.7.4	Verkkotunnuksen käyttäjän oikeudet	25
2.8	Ilmoitusvelvollisuus tietoturvahäiriöistä	26
2.8.1	Tietoturvahäiriöstä on ilmoitettava välittömästi.....	26
2.8.2	Merkittävät tietoturvaloukkaukset.....	27
2.9	Nimipalvelimet	29
2.9.1	Nimipalvelinmääritykset.....	30
2.9.2	Nimipalvelun tietoturvalaajennus DNSSEC	31
2.9.3	Nimipalvelintesti	33
2.10	Tekniset rajapinnat	33
2.10.1	Selainkäyttöliittymä	33
2.10.2	EPP-rajapinta	34
2.10.3	RFC-standardit	34
2.10.4	KATAKRI-vaatimukset käytettäessä EPP-rajapintaa	34
2.10.5	EPP-testiympäristö	36
2.10.6	Fi-verkkotunnusten whois-palvelu	36
2.10.7	Domain Availability Service (DAS)	36
2.10.8	OData	37
2.11	Välittäjäksi ilmoittautuminen	37
2.11.1	Lakisäeinen prosessiosoite ja muut sähköpostiosoitteet	37
2.11.2	Jälleenmyyjien välitystoiminta	38

1 Verkkotunnusvälittäjän tehtävät ja velvoitteet

1.1 Verkkotunnusvälittäjän palveluvelvoitteet

Verkkotunnusvälittäjä auttaa ja neuvoo asiakkaitaan fi-verkkotunnuksiin liittyvissä asioissa. Välittäjä rekisteröi fi-verkkotunnukset ja tekee niihin asiakkaidensa pyytämät muutokset.

Verkkotunnuksen käyttäjä asioi oman verkkotunnusvälittäjänsä kanssa kaikissa fi-verkkotunnuksiin liittyvissä tilanteissa. Välittäjällä on sähköisen viestinnän palveluista annetun lain säädösten myötä velvollisuus huolehtia, että käyttäjän oikeudet toteutuvat ja hän saa tarvitsemaansa tietoa fi-verkkotunnuksista sekä välittäjätoiminnan muutoksista.

Välittäjät hoitavat asiakkaidensa pyynnöstä fi-verkkotunnuksen

- rekisteröimisen Liikenne- ja viestintäviraston verkkotunnusrekisteriin
- tietojen päivittämisen
- voimassaoloajan uusimisen
- vaihtamisen välittäjältä toiselle
- siirron käyttäjältä toiselle
- irtisanomisen.

Välittäjä on myös velvollinen antamaan asiakkailleen

- yleistä neuvontaa fi-verkkotunnuksiin liittyen
- tiedon, mikäli välittäjätoiminta on päättynyt tai Liikenne- ja viestintävirasto on antanut välittäjää koskevan kieltopäätöksen.

1.1.1 Rekisteröimisestä ja uusimisesta maksaminen

Välittäjä maksaa asiakkaidensa verkkotunnusten rekisteröinneistä ja uusimisista Liikenne- ja viestintävirastolle välittäjän teknisen rajapinnan kautta. Verkkotunnuksen rekisteröimisen tai uusimisen hinta on voimassaoloajan mukaan:

- 1 vuosi 9 euroa
- 2 vuotta 18 euroa
- 3 vuotta 27 euroa
- 4 vuotta 36 euroa
- 5 vuotta 45 euroa.

Rekisteröinnit ja uusimiset vähennetään välittäjän ennakkomaksutililtä, jolle välittäjä varaa toimenpiteisiinsä rahaa. Välittäjä maksaa verkkotunnusmaksuista Liikenne- ja viestintäministeriön sähköisen viestinnän maksuasetuksen mukaisesti.

Liikenne- ja viestintävirasto ei palauta maksua välittäjälle, vaikka verkkotunnus olisi vahingossa väärin rekisteröity tai Liikenne- ja

viestintävirasto myöhemmin poistaisi verkkotunnuksen verkkotunnusrekisteristä päätöksellä.

1.2 Velvollisuus neuvoa asiakkaita

Verkkotunnusvälittäjän on neuvottava asiakkaitaan ennen fi-verkkotunnusten rekisteröimistä. Neuvontaa on annettava vähintään verkkotunnuksen muodosta, sisällöstä ja lainmukaisuudesta.

Verkkotunnusvälittäjän on tarjottava asiakkailleen tietoa fi-verkkotunnusten edellytyksistä vaivattomasti ja kattavasti ennen verkkotunnuksen rekisteröintiä. Velvollisuus rajoittuu tiedonantoon. Lopullinen vastuu verkkotunnuksen lainmukaisuudesta on verkkotunnuksen käyttäjällä.

Tietojen on oltava saatavilla niin nykyisille kuin tuleville verkkotunnusten käyttäjille riippumatta siitä, ovatko asiakkaat jo luoneet sopimussuhteen välittäjään vai eivät.

Välittäjän on aktiivisesti edesautettava verkkotunnusmerkintöjen lainmukaisuutta. Erityisesti suojattuihin nimiin ja tavaramerkkeihin liittyvien edellytysten tulee olla asiakkaiden tiedossa jo ennen verkkotunnusten rekisteröintiä. Neuvontavelvollisuuden tarkoituksena on välttää virheellisiä ja lainvastaisia verkkotunnusrekisteröintejä, jotka saattavat johtaa jopa verkkotunnuksen peruuttamiseen.

1.2.1 Neuvonnan vähimmäisvaatimukset

Välittäjän tiedonantovelvollisuuden toteuttamistapa on vapaa, mutta sisällöllisesti verkkotunnusvälittäjän on tarjottava asiakkailleen verkkotunnuksen sisältöön ja muotoon liittyen vähintään seuraavat tiedot:

Mikä on suojattu nimi tai tavaramerkki?

- Suojattuja nimiä ja merkkejä ovat sähköisen viestinnän palveluista annetun lain perusteella:
- Suomen kauppa-, tavaramerkki-, yhdistys-, säätiö- tai puolurekisteriin merkityt nimet tai merkit
- julkisyhteisön, valtion liikelaitoksen, itsenäisen julkisoikeudellisen laitoksen, julkisoikeudellisen yhdistyksen ja vieraan valtion edustuston ja sen toimielimien nimet
- toiminimi- ja tavaramerkkilaisissa tarkoitetut vakiintuneet nimet, toissijaiset tunnuksot tai tavaramerkit
- EUIPO:n tavaramerkkirekisteriin merkityt EU-tavaramerkit.

Mistä voi tarkastaa suojatut nimet ja tavaramerkit?

Välittäjän on tarjottava asiakkailleen linkit Patentti- ja rekisterihallituksen (PRH) julkisiin rekistereihin (yritys- ja yhteisötietojärjestelmä,

yhdistysrekisteri, tavaramerkkirekisteri) sekä Euroopan unionin immateriaalioikeusviraston (EUIPO) EU-tavaramerkkirekisteriin.

Mitä tarkoittaa verkkotunnuksen lainmukaisuus?

Verkkotunnus ei saa merkitsemishetkellä

- vastata toisen suojattua nimeä tai merkkiä, ellei verkkotunnuksen käyttäjä pysty esittämään hyväksyttävää perustetta verkkotunnuksen rekisteröinnille
- muistuttaa toisen suojattua nimeä tai merkkiä, jos verkkotunnus rekisteröidään ilmeisessä hyötymis- tai vahingoittamistarkoituksessa.

Verkkotunnuksessa sallitut merkit

Välittäjän on neuvottava asiakkaitaan verkkotunnuksissa sallituista merkeistä, joita ovat kirjaimet a-z ja numerot 0-9. Lisäksi sallittuja merkkejä ovat kansalliset merkit å, ä ja ö sekä Suomessa puhuttavan saamen kielen merkit ja lisäksi tavuviiva-miinusmerkki.

Välittäjien on huomioitava kansallisia merkkejä sisältäviin verkkotunnuksiin kohdistuvat rajoitukset markkinoidessaan ja välittäessään verkkotunnuksia. Verkkotunnusta hakevien ja harkitsevien asiakkaiden tulee tietää kansallisia merkkejä sisältävien tunnusten teknisistä rajoitteista.

Erityisesti on huomioitava asiakkaan mahdollinen tarve hakea sekä kansallisia merkkejä sisältävä verkkotunnus että vastaava verkkotunnus ilman kansallisia merkkejä, esimerkiksi ääkkönen.fi ja aakkonen.fi.

Latinalaisten aakkosten ulkopuolisten kirjoitusmerkkien käytön mahdollistaa punycode, josta käytetään myös nimeä ACE (ASCII Compatible Encoding). Nimipalvelinjärjestelmä ymmärtää kansallisia merkkejä sisältävän verkkotunnuksen, jos se on määritelty teknisesti ACE-muotoon.

Esimerkiksi ääkkönen.fi on ACE-muotoisena: xn--kknen-fraa=0m.fi.

Muunnostyökaluja tarjoavia verkkosivuja on lukuisia. Sellainen löytyy myös Liikenne- ja viestintäviraston sivustolta.

1.3 Tietojen oikeellisuudesta ja ajantasaisuudesta huolehtiminen

Välittäjä pitää asiakkaidensa tiedot ajan tasalla fi-verkkotunnusrekisterissä sekä rekisteröintihetkellä että myöhemmin tietojen muuttuessa.

Fi-verkkotunnus rekisteröidään aina sen todellisen käyttäjän nimiin. Asiakkaan fi-verkkotunnusta ei saa esimerkiksi merkitä verkkotunnusvälittäjän omiin nimiin. Liikenne- ja viestintäviraston selvittäessä fi-verkkotunnuksiin liittyviä epäselvyyksiä tai riitoja arvioidaan aina verkkotunnusrekisteriin käyttäjäksi merkityn oikeuksia suhteessa muiden oikeuksiin.

Verkkotunnusvälittäjän asiakkaan oikeusturvan kannalta on erittäin tärkeää, että käyttäjämerkintä on totuudenmukainen ja verkkotunnus on rekisteröity oikealle taholle.

Verkkotunnusrekisterissä on oltava oikea ja ajantasainen tieto myös rekisteröintihetken jälkeen. Asiakkaan esittäessä välittäjälleen pyynnön tehdä muutoksia verkkotunnukselle, on välittäjä velvollinen toteuttamaan seuraavat muutokset:

- verkkotunnuksen käyttäjän yhteystietojen päivittäminen
- verkkotunnuksen irtisanominen
- verkkotunnuksen siirtäminen toiselle käyttäjälle
- verkkotunnuksen välittäjän vaihtaminen
- verkkotunnuksen uusiminen.

1.3.1 Yhteystietojen päivittäminen

Välittäjän on pidettävä fi-verkkotunnusasiakkaansa tiedot ajantasaisina. Yhteystiedot on päivitettävä asiakkaan pyytäessä ja muissakin tilanteissa oma-aloitteisesti.

Oikeiden käyttäjätietojen ilmoittaminen ja ylläpitäminen ajantasaisina on verkkotunnusvälittäjän vastuulla. Mikäli verkkotunnuksen käyttäjälle (eli verkkotunnusvälittäjän asiakkaalle) aiheutuu vahinkoja välittäjän laiminlyönnistä, voi käyttäjä vaatia vahingonkorvauksia.

1.3.2 Lakisääteinen prosessiosoite ja muut sähköpostiosoitteet

Liikenne- ja viestintävirasto käyttää kuulemisiin ja tiedoksiantoihin verkkotunnusrekisteriin merkittyä sähköpostiosoitetta, jolloin verkkotunnuksiin liittyvä asiakirja tai päätös voidaan aina antaa tiedoksi sähköpostilla. Tämän ns. prosessiosoitteen oikeudellinen merkitys on huomattava ja sen ilmoittaminen Liikenne- ja viestintävirastolle on pakollista.

Prosessiosoitteen käyttö mahdollistaa Liikenne- ja viestintäviraston velvoittavien päätösten nopean tiedoksiannon, sillä päätös tai muu asiakirja katsotaan annetun tiedoksi kolmantena päivänä viestin lähettämisestä.

Verkkotunnuksen käyttäjän prosessiosoitteen oikeellisuus on merkittävä tieto, jonka ajantasaisuus on erittäin tärkeää välittäjän oman oikeusturvankin kannalta. Välittäjän vastuulla on ilmoittaa verkkotunnuksen käyttäjän prosessiosoite ja pitää se ajantasaisena.

Liikenne- ja viestintäviraston sähköiseen järjestelmään voi ilmoittaa muitakin sähköpostiosoitteita, jos verkkotunnusvälittäjä pitää tarpeellisena esimerkiksi erottaa verkkotunnusta koskevien päivittäisten teknisluonteisten asioiden käsittelyyn käytettävät sähköpostiosoitteet pakollisesta prosessiosoitteesta.

1.4 Verkkotunnuksen uusiminen

Välittäjä tiedottaa fi-verkkotunnuksen käyttäjää verkkotunnuksen voimassaoloajan päättymisestä.

Verkkotunnusrekisteriin merkitty verkkotunnus on voimassa vähintään yhden vuoden ja enintään viisi vuotta. Verkkotunnusvälittäjä voi uusia verkkotunnusta koskevan merkinnän yhdeksi, kahdeksi, kolmeksi, neljäksi tai viideksi vuodeksi kerrallaan.

1.4.1 Välittäjän velvollisuudet verkkotunnuksen voimassaoloajan päättyessä

Kun fi-verkkotunnuksen voimassaoloaika on päättymässä, verkkotunnusvälittäjä

- tiedottaa voimassaoloajan päättymisestä käyttäjää hyvissä ajoin
- antaa käyttäjälle ohjeet, miten verkkotunnuksen uusimispyynnön voi tehdä
- selvittää käyttäjälle, mitä uudistamatta jättämisestä seuraa.

Verkkotunnusvälittäjä ja verkkotunnuksen käyttäjä (asiakas) voivat sopia verkkotunnuksen uusimisesta sopimuksella. Voidaan esimerkiksi sopia, että välittäjä huolehtii asiakkaansa verkkotunnuksen voimassaolosta automaattisesti ja uusii verkkotunnuksen vuosittain ilman erillistä tiedottamista verkkotunnuksen voimassaoloajan päättymisestä.

Liikenne- ja viestintäviraston valtuuksiin eivät kuulu verkkotunnuksen käyttäjän ja verkkotunnusvälittäjän välisten sopimusten valvonta tai sopimusriitojen ratkaiseminen.

1.5 Verkkotunnuksen irtisanominen

Fi-verkkotunnuksen käyttäjä voi halutessaan irtisanoa verkkotunnuksensa ennen voimassaolon päättymistä. Välittäjä poistaa pyynnöstä verkkotunnuksen Liikenne- ja viestintäviraston rekisteristä.

Verkkotunnuksen irtisanomisesta (eli poistamisesta fi-verkkotunnusrekisteristä ja fi-juuresta) huolehtii verkkotunnusvälittäjä. Irtisanominen suoritetaan verkkotunnuksen käyttäjän pyynnöstä.

Verkkotunnusvälittäjä on vastuussa siitä, että

- verkkotunnus irtisanoaan vain verkkotunnuksen käyttäjän tai tämän valtuuttaman asiamiehen pyynnöstä
- mikään ulkopuolinen taho ei tahallaan tai tahattomasti irtisano verkkotunnuksia
- verkkotunnuksen käyttäjän ollessa organisaatio, varmistutaan siitä, että irtisanojalla on oikeus irtisanomiseen (esim. kaupparekisteriin merkitty yrityksen nimenkirjoitusoikeus).

1.5.1 Irtisanomisen ongelmatilanteet

Verkkotunnuksen virheellisellä irtisanomisella voi olla huomattavia taloudellisia vaikutuksia. Välittäjä voi vakavimmillaan joutua virheellisestä irtisanomisesta vahingonkorvausvastuuseen.

Verkkotunnuslainsäädäntö ei ota kantaa verkkotunnuksen käyttäjän ja verkkotunnusvälittäjän väliseen sopimussuhteeseen, vaan irtisanomisesta aiheutuvat sopimus-, vahingonkorvaus- tai kuluttajaoikeudelliset kysymykset ratkaistaan muun lainsäädännön nojalla.

1.6 Verkkotunnuksen siirtäminen uudelle käyttäjälle

Välittäjä siirtää fi-verkkotunnuksen uudelle käyttäjälle varmistuttuaan siitä, että siirtopyynnön esittää siihen oikeutettu taho.

Verkkotunnuksen käyttäjä voi halutessaan siirtää voimassa olevan verkkotunnuksensa toiselle käyttäjälle. Siirtopyynnön saatuaan verkkotunnusvälittäjä

- varmistaa, että pyytäjällä on oikeus siirtää verkkotunnus
- lähettää verkkotunnuksen siirtoavaimen verkkotunnuksen käyttäjälle näkemättä avainkoodin sisältöä
- siirtää verkkotunnuksen viiden arkipäivän kuluessa käyttäjältä toiselle, kun siirtoavain on toimitettu välittäjälle.

Käyttäjän on valtuutettava välittäjä tekemään siirto antamalla siirtoavain tälle tiedoksi. Näin varmistetaan verkkotunnuksen käyttäjän suostumus verkkotunnuksen siirtoon ja se, ettei välittäjä voi siirtää verkkotunnusta ilman käyttäjän todellista suostumusta.

Käyttäjä voi valtuuttaa siirron tekijäksi joko oman välittäjänsä tai verkkotunnuksen vastaanottajan välittäjän. Verkkotunnuksen vastaanottajan välittäjä pystyy tekemään siirron vain, jos tälle on luovutettu siirtoavaimen lisäksi myös välittäjän vaihtoavain, jolla tämä on jo ottanut verkkotunnuksen hallintaansa.

Siirtoavain on Liikenne- ja viestintäviraston määrittelemä koodi, jota välittäjä ei näe eikä määrittele. Siirtoavain lähetetään aina verkkotunnuksen nykyiselle käyttäjälle, jonka on itse annettava se välittäjälle verkkotunnuksen siirtoa varten.

1.6.1 Oikeus tehdä verkkotunnuksen siirtopyyntö

Verkkotunnusvälittäjän on varmistuttava siitä, ettei kukaan muu kuin verkkotunnuksen käyttäjä tai tämän valtuuttama asiamies pyydä siirtoa. Verkkotunnuksen siirtäminen on käyttäjän oikeusturvan kannalta merkittävä toimenpide, ja verkkotunnusvälittäjällä on velvollisuus toteuttaa toimenpide huolellisesti. Myös verkkotunnuksen vastaanottajalla (uusi

käyttäjä) on lähtökohtaisesti oikeus luottaa siihen, että siirrolle on laillinen peruste.

Mikäli jokin muu taho kuin verkkotunnuksen käyttäjä pyytää siirtoa, on verkkotunnusvälittäjän vaadittava käyttäjän antama valtuutus siitä, että siirtopyynnön esittänyt taho on oikeutettu toimimaan käyttäjän puolesta.

1.6.2 Verkkotunnuksen siirtoaika

Verkkotunnusvälittäjän on toteutettava siirto teknisesti viiden arkipäivän kuluessa siitä, kun verkkotunnuksen vanha käyttäjä on toimittanut verkkotunnusvälittäjälle siirtoavaimen ja uuden käyttäjän tiedot. Aikaraja on lakisääteinen palvelutasovaatimus.

1.7 Välittäjän vaihtaminen

Fi-verkkotunnuksen käyttäjän halutessa vaihtaa välittäjää, osallistuu vanha välittäjä vaihtoprosessiin luomalla välittäjän vaihtoavaimen ja antamalla sen tiedoksi käyttäjälle tai suoraan uudelle välittäjälle.

Verkkotunnuksen käyttäjä voi vapaasti vaihtaa verkkotunnusvälittäjää. Verkkotunnusvälittäjän vaihtaminen ei edellytä erityistä syytä.

Välittäjän vaihtamisen vaiheet

1. Halutessaan vaihtaa verkkotunnusvälittäjää verkkotunnuksen käyttäjän tulee joko
 - valtuuttaa uusi välittäjä hankkimaan välittäjän vaihtoavaimen vanhalta välittäjältä tai
 - pyytää itse välittäjän vaihtoavaimen vanhalta välittäjältä ja saatuaan avaimen, toimittaa se edelleen uudelle välittäjälle.
 - Verkkotunnusvälittäjän vaihtamista koskeva pyyntö on tehtävä välittäjälle kirjallisesti, jotta avaimen toimittamisen määräajan kulumisen tai muut epäselvyydet on mahdollista selvittää jälkikäteen.
2. Vanhan verkkotunnusvälittäjän on varmistettava, että käyttäjällä tai uudella verkkotunnusvälittäjällä on oikeus pyytää välittäjän vaihtoavaimen ja toimitettava se pyytäjälle viiden arkipäivän kuluessa oikeutetusta pyynnöstä.

Vanhalta välittäjältä edellytetään huolellisuutta sen varmistamiseksi, ettei välittäjän vaihtoa pyydä muu kuin verkkotunnuksen käyttäjäksi merkitty taho. Mikäli pyynnön esittää jokin muu taho, on pyynnön esittäjän osoitettava riittävä valtuutus. Verkkotunnusvälittäjä voi tarvittaessa esimerkiksi ottaa yhteyttä käyttäjään asian varmistamiseksi.

- Uusi välittäjä saa käyttäjän pyyntötavasta riippuen välittäjän vaihtoavaimen joko vanhalta välittäjältä tai käyttäjältä, jonka jälkeen uusi välittäjä voi ottaa verkkotunnuksen hallintaansa.

1.7.1 Välittäjän vaihtoavain

Välittäjän vaihtoavaimella tarkoitetaan koodia, jonka avulla verkkotunnuksen hallinnointi voidaan siirtää verkkotunnusvälittäjältä toiselle. Koodin luo vanha välittäjä verkkotunnusjärjestelmässä ja ottaa sen sieltä talteen. Järjestelmä ei lähetä koodia, vaan välittäjä toimittaa sen haluamallaan tavalla esim. puhelimitse tai sähköpostitse uudelle välittäjälle. Vanhalla välittäjällä tarkoitetaan verkkotunnuksen hallinnoinnista luopuvaa välittäjää ja uudella välittäjällä verkkotunnuksen hallinnoinnin vastaanottavaa välittäjää.

1.7.2 Verkkotunnus ilman välittäjää

Välittäjän vaihtoavainta tarvitaan myös, kun verkkotunnukselta puuttuu välittäjä. Verkkotunnuksen käyttäjän on tällöin pyydettävä koodi Liikenne- ja viestintävirastolta. Saatuaan koodin verkkotunnuksen käyttäjä toimittaa sen valitsemalleen välittäjälle, joka liittää verkkotunnuksen hallintaansa.

1.7.3 Ongelmatilanteet

Verkkotunnuksen käyttäjän saatettua verkkotunnusvälittäjänsä tietoiseksi halustaan vaihtaa verkkotunnusvälittäjää, on välittäjän suoritettava vaihtamisen edellytyksenä olevat toimenpiteet kohtuullisessa ajassa (viisi arkipäivää), ja edesautettava vaihdon toteutumista.

Jos vanha verkkotunnusvälittäjä ei ole toimittanut välittäjän vaihtoavainta uudelle välittäjälle tai käyttäjälle määräajassa toistuvista pyynnöistä huolimatta, uusi verkkotunnusvälittäjä voi pyytää Liikenne- ja viestintävirastoa toimittamaan välittäjän vaihtoavaimen käyttäjälle.

Verkkotunnuksen käyttäjän ja verkkotunnusvälittäjän välinen sopimussuhde ei ole verkkotunnuslainsäädännön piirissä, vaan verkkotunnuksen siirrosta tai välittäjän vaihtamisesta aiheutuvat sopimus- tai kuluttajaoikeudelliset kysymykset ratkaistaan muun lainsäädännön nojalla.

1.8 Välitystoiminnan päättyessä

Välittäjän toiminnan päättyessä on siitä tiedotettava Liikenne- ja viestintävirastolle ja asiakkaille. Myös Liikenne- ja viestintäviraston antamasta toiminnanharjoittamisen kieltopäätöksestä on ilmoitettava omille asiakkailleen.

Verkkotunnusvälittäjän toiminnan lopettamisesta on ilmoitettava Liikenne- ja viestintävirastolle ja välittäjän omille asiakkaille viimeistään kaksi viikkoa etukäteen, jotta välittäjän asiakkailta (fi-verkkotunnusten käyttäjillä) on

mahdollisuus säilyttää verkkotunnuksensa toimintakuntoisena ja varmistaa, että he ehtivät vaihtaa nimipalvelimien ylläpitäjän ennen verkkotunnusvälittäjän toiminnan loppumista.

Ilmoitukset toiminnan lopettamisesta on tehtävä asiakaskohtaisesti. Tiedottaminen esimerkiksi pelkästään verkkotunnusvälittäjän internetsivuilla ei ole riittävää, vaikkakin toissijaisena tapana suositeltavaa. Asiakkaille viestiminen sähköpostitse on tehokasta, mutta on hyvä pyrkiä tavoittamaan asiakkaat myös puhelimitse.

Liikenne- ja viestintävirasto suosittelee, että sekä välitystoiminnan päättyessä että väliaikaisesti keskeytyessä välittäjä hoitaa tiedottamisen hyvissä ajoin asiakaskohtaisesti.

1.8.1 Liikenne- ja viestintäviraston kieltopäätöksestä ilmoittaminen

Liikenne- ja viestintävirasto valvoo verkkotunnusvälitystoiminnan lainmukaisuutta ja huomauttaa tarvittaessa laiminlyönneistä. Välitystoiminta voi keskeytyä määräajaksi Liikenne- ja viestintäviraston päätöksellä, jos välittäjä ei korjaa virhettään tai laiminlyöntiään Liikenne- ja viestintäviraston huomautuksista huolimatta.

Mikäli Liikenne- ja viestintävirasto antaa välittäjälle toiminnanharjoittamista koskevan kieltopäätöksen, on välittäjän ilmoitettava siitä omille asiakkailleen viipymättä, koska välittäjän asiakkaat voivat tällaisissa tilanteissa joutua etsimään uuden verkkotunnusvälittäjän.

Liikenne- ja viestintävirasto toimeenpanee kieltopäätöksen sulkemalla verkkotunnusvälittäjän teknisen rajapinnan joko siten

- ettei välittäjä voi enää rekisteröidä uusia verkkotunnuksia tai
- ettei välittäjä lisäksi voi edes ylläpitää asiakkaidensa olemassa olevia verkkotunnuksia.

1.8.2 Ennakkomaksutilin sulkeminen

Välitystoimintansa lopettanut välittäjä voi pyytää Liikenne- ja viestintävirastoa palauttamaan ennakkomaksutililleen tallettamansa rahan, joka on jäänyt käyttämättä verkkotunnusten rekisteröimiseen ja uusimiseen.

2 Välitystoiminnan tietoturva

Välittäjän on huolehdittava tietoturvasta varautumalla uhkiin ja puuttamalla poikkeamiin. Tietoturvan vähimmäisvaatimukset turvaavat sekä välitystoimintaa että verkkotunnuskäyttäjän oikeuksia.

Tietoturvallisuuden eri osa-alueiden huomioiminen on tärkeää kaikissa fi-verkkotunnusten välitystoiminnan vaiheissa: suunniteltaessa, ylläpidettäessä ja lopetettaessa välityspalvelua. Jotta tietoturvasta

huolehtiminen olisi rutiininomaista ja jokapäiväistä, se vaatii tuekseen prosesseja ja käytäntöjä.

Varautumissuunnitelma on dokumentoitava

Verkkotunnusvälittäjän velvollisuutena on määritellä yksityiskohtaiset ohjeet tietoturvaohjeiden varalle. Verkkotunnusvälittäjän on varmistuttava siitä, että

- tietoturvallisuuden kannalta merkittävät tapahtumat havaitaan
- havaittuihin ongelmatilanteisiin ja tietoturvapoikkeamiin puututaan.

Kun tietoturvaa tukevien suunnitelmien dokumentointi on ajan tasalla, on välittäjällä perusta tietoturvansa hallinnalle ja kehittämiselle. Dokumentoinnin perusteella myös Liikenne- ja viestintävirasto voi tarvittaessa todentaa, että välittäjä noudattaa tietoturvavelvoitteita. Yrityksen toiminnan laajuudesta riippuu, miten tietoturva-asiat on järkevintä dokumentoida.

Tietoturvalle on asetettu vähimmäisvaatimukset

Tietoturvalla tarkoitetaan sähköisen viestinnän palveluista annetun lain (3.1 §:n 28 kohta) mukaan hallinnollisia ja teknisiä toimia tietojen luottamuksellisuuden, eheyden ja saatavuuden turvaamiseksi. Niiden avulla varmistetaan, että

- tiedot ja tietojärjestelmät ovat vain niiden käyttöön oikeutettujen hyödynnettävissä
- tietoja eivät voi muuttaa muut kuin siihen oikeutetut tahot.

Liikenne- ja viestintäviraston Verkkotunnusmääräyksessä 68 kuvataan tietoturvan hallinnoinnin vähimmäisvaatimukset, jotka verkkotunnusvälittäjän tulee toteuttaa toiminnassaan. Vaatimuksilla

- turvataan välitystoiminnan tietoturvan perustaso.
- pienennetään tietoturvariskien aiheuttamia vahingollisia vaikutuksia välitystoiminnalle ja fi-verkkotunnusten käyttäjille.

2.1 Tietoturva käytännössä

Verkkotunnusvälittäjän on dokumentoitava ja ylläpidettävä ajantasaista kuvausta siitä, miten se huomioi toiminnassaan tietoturvan eri osa-alueet.

Tietoturvallisuuden toteuttamisessa ja sitä kuvaavissa asiakirjoissa on huomioitava useita eri asiakokonaisuuksia, jotka on lueteltu Liikenne- ja viestintäviraston määräyksessä 68. Määräys ei aseta tarkkoja vaatimuksia tietoturvan toteuttamiselle, koska tarkoituksenmukainen toteutus voi vaihdella yrityksen tarjoamien palvelujen perusteella.

Oleellista on, että verkkotunnusvälittäjä tunnistaa omaan toimintaansa kohdistuvat tietoturva-vaatimukset ja niiden toteuttamiseksi tarvittavat käytännöt fi-verkkotunnusten välitystoiminnassa.

Liikenne- ja viestintävirasto edellyttää, että verkkotunnusvälittäjä ylläpitää dokumentaatiota siitä, miten se toteuttaa tietoturvaa toiminnassaan. Liikenne- ja viestintävirasto ei yksilöi vaadittuja dokumentteja erikseen, vaan kokonaisuus on välittäjän oman harkinnan varainen. Oleellista on, että dokumentointi on ajantasaista, ja sen avulla voi todeta, että kaikki pykälässä luetellut tietoturvan osa-alueet on huomioitu välitystoiminnassa.

2.1.1 Tietoturvan osa-alueet

Verkkotunnusvälittäjän on otettava fi-verkkotunnusten välitystoiminnan eri vaiheissa huomioon seuraavat tietoturvan osa-alueet:

Hallinnollinen tietoturvallisuus

- tietoturvallisuuden ohjausasiakirjat (tyypillisesti esim. tietoturvapoliittikka ja -arkkitehtuuri), joilla organisaation johto osoittaa tietoturvallisuuden tahtotilan, yleiset periaatteet ja sitoutumisensa tietoturvan toteuttamiseen
- prosessit ja niiden hallinta
- riskien hallinta ja jatkuvuuden turvaaminen (ks. Liikenne- ja viestintäviraston määräys 68, 15 §)
- dokumentointikäytännöt ja -järjestelmät
- auditointi- ja harjoitusmenettelyt.

Henkilöstöturvallisuus

- henkilöiden tietoturva-vaastuut ja velvollisuudet
- henkilöstön tietoturvaosaaminen ja sen kehittäminen
- henkilöiden taustatarkastukset
- avainhenkilöriskit
- vaarallisten vastuu- ja tehtäväkokonaisuuksien estäminen
- tehtäväkierto väärinkäytösten havaitsemiseksi
- työsuhteen päättyessä noudatettava menettely
- henkilöstön väärinkäytökset ja ohjeistuksen vastaiset toimet.

Laitteisto-, ohjelmisto- ja tietoliikenneturvallisuus

- haavoittuvuuksien hallinta
- tietoturvaloukkausten havainnointi (ks. Määräys 68, 17 - 18 §:t)
- muutostenhallinta (ks. Määräys 68, 19 §).
- tietoaineisto- ja käyttöturvallisuus
- tietojen luottamuksellisuuden, eheyden ja saatavuuden varmistaminen
- tietoaineistojen luokittelu ja luokituksen mukainen käsittely (ks. Määräys 68, 16 §)
- käyttöoikeusrekisterin ylläpitovastuut: käyttöoikeuksien jakaminen, muuttaminen ja poistaminen

- käyttöoikeuksien kasaantumisen estäminen
- asiaankuulumattomien pääsyn estäminen verkkotunnusten välityspalvelun toteuttamiseen liittyviin hallinta- ja konfiguraatietietoihin sekä verkkotunnusvälittäjän asiakkaiden veloitus-, asiakas- ja lokitietoihin
- tietoineistojen säilytys ja tuhoaminen.

Fyysinen turvallisuus

- tilojen sijainti ja ympäristön turvallisuus
- pääsynhallinta
- rakenteellinen suojaaminen.

Tarvittaessa Liikenne- ja viestintävirastolla on oikeus auditoida verkkotunnusvälittäjän välitystoimintaa.

Liikenne- ja viestintäviraston määräykset löytyvät viraston verkkosivuilta.

2.2 Riskien hallinta

Verkkotunnusvälittäjän on tunnistettava välitystoimintansa jatkuvuuden kannalta tärkeät toiminnot, tiedot ja järjestelmät sekä arvioitava ja käsiteltävä säännöllisesti niihin kohdistuvat tietoturvariskit ja niiden hallinta. Riskien hallinnan prosessit ja tulokset on dokumentoitava.

Turvallisuusriskillä tarkoitetaan jonkinlaisen haitan tai vaurion todennäköisyyttä ja sen seurauksia. Tietoturvariskeillä tarkoitetaan sellaista tahatonta tai tahallista tekijää, joka vaarantaa verkkotunnusten välitystoiminnan luottamuksellisuutta, eheyttä tai saatavuutta. Tietoturvariskin erottaa tietoturvauhasta sillä, että sen todennäköisyyttä ja vaikutuksia on arvioitu.

Tietoturvariskit voivat aiheutua esimerkiksi:

- inhimillisistä virheistä
- henkilöstölle annettujen ohjeiden puutteista tai noudattamatta jättämisestä
- varkauksista tai ilkivallasta
- laitteiden, järjestelmien tai ohjelmistojen virheistä ja toimintahäiriöistä
- haittaohjelmien leviämisestä
- tietoineistojen tuhoutumisesta
- tulipalosta tai vesivahingosta
- alihankkijan tai kumppanuusverkostoon kuuluvan toimijan virheistä ja laiminlyönneistä.

Riskien hallinnan tavoitteet

Riskien hallinta on prosessi, jonka tarkoitus on tunnistaa riskejä, vähentää niiden todennäköisyyttä ja/tai vaikutuksia hyväksyttävälle tasolle ja ylläpitää saavutettua tasoa. Riskien hallinnan tehtävänä on suojella

organisaatiota ja sen kykyä suorittaa toimintojaan taloudelliset seikat huomioon ottaen.

Riskien hallinnan vaatimuksilla pyritään varmistamaan, että verkkotunnusvälittäjä on tietoinen riskien mahdollisen toteutumisen aiheuttamista seurauksista ja siitä, ovatko riskiä pienentävät toimenpiteet riittäviä.

Riskien hallinnan tavoitteena on muun muassa:

- nopeuttaa tietoturvaongelmista toipumista
- vähentää tietoturvaongelmista aiheutuneita kustannuksia ja vahinkoja
- kohdentaa verkkotunnusten välitystoiminnan tietoturvallisuutta parantavia investointeja
- parantaa verkkotunnusten välitystoiminnan laatua ja tuottavuutta
- optimoida taloudellisesti verkkotunnusten välitystoimintaan kohdistuvien riskien hallintaa ja ennaltaehkäistä riskien toteutumista.

Riskien tunnistaminen ja käsittely

Riskien hallinnasta on laadittu mm. seuraavia standardeja ja julkaisuja:

- ISO/IEC 27005
- NIST 800- 30 Risk Management Guide
- OCTAVE

Liikenne- ja viestintävirasto ei aseteta velvoitetta tietyn standardin noudattamiselle. Riskienhallintamallit vaihtelevat yrityksittäin eikä yhtä jokaiselle sopivaa mallia ole olemassa.

Liikenne- ja viestintävirasto edellyttää, että verkkotunnusvälittäjä tunnistaa omaan välitystoimintaansa ja sen jatkuvuuteen liittyvät riskit ja käsittelee ne. Käsittely tarkoittaa sitä, että verkkotunnusvälittäjä määrittää toiminnalleen hyväksyttävän riskitason ja toteuttaa tarkoituksenmukaisin keinoin (usein ns. kontrollein) tämän tason. Käytännössä riskien hallinnan tulee siis olla vastuutettua ja aikataulutettua. Lisäksi riskien hallinnan toteutumista ja vaikutuksia tulee seurata.

Liikenne- ja viestintävirasto edellyttää myös, että riskien hallinta on säännöllistä eli että riskejä ja niiden hallintakeinoja arvioidaan säännöllisesti. Verkkotunnusvälittäjä voi itse määrittää sopivat seurantajaksot. Tyypillisesti riskiarviointia tehdään yrityksissä

- säännönmukaisesti vuosittain
- määriteltäessä uusia palveluja tai toimintoja
- mahdollisen riskin realisoitumisen jälkeen.

Prosessin ja tulosten dokumentointi

Liikenne- ja viestintävirasto valvoo verkkotunnusvälittäjien toimintaa ja välittäjien on riskien hallinnan vaatimusten noudattamisen valvomiseksi dokumentoitava määrittämänsä riskien hallinnan prosessi ja tulokset.

2.3 Tietoaineistot

Verkkotunnusvälittäjällä on oltava käytössä välitystoiminnan kannalta tärkeiden tietoaineistojen luokitusjärjestelmä ja luokitteluun liittyvä tietoaineistojen käsittelymenettely.

Tietoaineistojen luokitusjärjestelmä ja käsittelymenettely varmistavat, että verkkotunnusten välitystoimintaan liittyvät tärkeät tiedot ovat vain niiden käyttöön oikeutettujen saatavilla. Luokituskriteereistä ja käsittelymenettelyistä on laadittava ja ylläpidettävä ajantasainen dokumentaatio.

2.3.1 Aineistojen luokittelu ja käsittely

Verkkotunnusvälittäjän on määriteltävä omaan toimintaansa soveltuva tietoaineistojen luokittelukriteeristö. Aineistot voi esimerkiksi luokitella seuraavasti:

- julkinen
- luottamuksellinen
- salainen.

Lisäksi verkkotunnusvälittäjän on määriteltävä se, miten välittäjä käsittelee (suojaa) eri luokkiin luokiteltuja aineistoja.

2.3.2 Tietoaineistodokumentit

Luokitus ja siihen liittyvä käsittelyohje on dokumentoitava. Luokituksen määrittelyssä ja sen dokumentoinnissa huomioitavia tekijöitä ovat esimerkiksi:

- yleiset periaatteet tietoaineiston turvaluokan ja luottamuksellisuuden arvioimiseksi ja tietoaineistojen salassa pysymiseksi
- käsittely- ja muutosoikeudet tietoaineiston lukuoikeuksien jakamisesta, muutosoikeuksista sekä näiden oikeuksien jakamisesta
- luottamuksellisuusluokan määrittäminen
- tiedon tai asiakirjan julkisuus: esimerkiksi asiasta puhuminen julkisesti
- asiakirjan ominaisuudet: paperi, leima ja muut merkinnät
- säilytys ja salaaminen
- tulostaminen ja kopiointi
- varmuuskopiointi
- vastaanottaminen, jakaminen, lähettäminen ja kuljettaminen
- tietojen ja asiakirjan käsittelyn dokumentoiminen
- asiakirjan arkistointi, käsittely tai käsittelyoikeuksien päättyminen
- tietojen ja asiakirjan hävittäminen.

2.4 Tietoturvan valvonta

Verkkotunnusvälittäjän on valvottava jatkuvasti välitystoimintaansa. Valvonnan avulla toimintaa häiritsevät tai uhkaavat tilanteet voidaan joko havaita tai kokonaan ennaltaehkäistä.

Verkkotunnusvälittäjän on varmistettava, että tietoturvallisuuden kannalta merkittävät tapahtumat havaitaan. Edellytyksenä välitystoiminnan valvomiselle on, että verkkotunnusten välitystoimintaan kohdistuvat tietoturvaloukkaukset ja -uhat voidaan havaita. Tämä tarkoittaa käytännössä sitä, että verkkotunnusvälittäjän tulee ylläpitää palvelunsa hallintajärjestelmää.

2.4.1 Uhkien havainnointi

Verkkotunnusvälittäjän oma-aloitteinen ja ripeä toiminta erilaisten häiriöiden havaitsemiseksi on tärkeää. Havainnointikyvyn avulla verkkotunnusvälittäjä pystyy aloittamaan tietoturvan häiriötilanteiden selvittämisen-, rajoittamisen- ja korjaamistoimenpiteet nopeasti, eikä sen tarvitse odottaa asiakasvalituksia.

Verkkotunnusvälittäjän tulee jatkuvasti valvoa välitystoiminnan tietoturvan tilaa. Valvonnan tulee tapahtua välitystoimintaan soveltuvalla hallintamekanismilla, joka havaitsee mahdollisimman nopeasti tietoturvan tilaa häiritsevät ongelmat. Esimerkkejä tällaisista tilanteista ovat

- palvelunestohyökkäykset
- tietovuodot
- tietomurron yritykset
- liian laajat käyttövaltuudet.

2.4.2 Uhkien ennaltaehkäisy

Tietoturvan häiriötilanteiden ennaltaehkäisyllä pyritään mahdollisimman varhaisessa vaiheessa havaitsemaan pienetkin tunnusmerkit alkavasta ongelmatilanteesta. Ennalta ehkäisemällä vaikutukset verkkotunnusten välitystoimintaan voidaan minimoida. Parhaimmillaan vaikutuksia ei näy palvelussa lainkaan.

Verkkotunnusvälittäjän tulee pyrkiä havaitsemaan ongelmiksi kehittymässä olevat tilanteet palvelunhallintamekanismiensa avulla. Mekanismeja voivat olla esimerkiksi:

- ohjelmistohälytykset ja palvelun laatumittarit, jotka ilmaisevat poikkeamat normaalitoiminnasta, vaikka eivät indikoikaan välitöntä häiriötä. Käyttökelpoisten hälytysten ja mittarien määrittely on verkkotunnusvälittäjän omalla vastuulla.
- ilmoitukset havaituista laitteisto- tai ohjelmistohaavoittuvuuksista, jotka ennakoivat tietoturvaongelmia.

2.4.3 Valvonnan dokumentointi

Välitystoiminnan valvontamekanismeista on laadittava ja ylläpidettävä ajantasaista dokumentaatiota, jotta verkkotunnusvälittäjä pystyy tarvittaessa osoittamaan, millä keinoin se täyttää annetut vaatimukset.

Erilaisten hälytys- ja ilmoitustietojen vastaanottoon ja analysointiin käytetyt järjestelmät ja menettelyt on dokumentoitava ja dokumentointia on ylläpidettävä. Toisin sanoen verkkotunnusvälittäjällä on oltava kuvaus siitä, millä teknisillä järjestelmillä ja millaisin toimenpitein se käsittelee palvelunsa tilasta kertovia tietoa tai niitä koskevia ilmoituksia.

2.5 Uhka- ja häiriötilanteiden hallinta

Verkkotunnusvälittäjän on laadittava ohjeet oman välitystoimintansa tietoturvaa uhkaavien tai häiritsevien tilanteiden varalle. Ohjeiden avulla sekä minimoidaan että selvitetään tilanteita.

Verkkotunnusvälittäjän on laadittava etukäteen selkeät menettelyohjeet, välitystoiminnan tietoturvaa häiritsevien tai uhkaavien tilanteiden selvittämiseksi. Ohjeiden avulla minimoidaan edellä mainittujen tilanteiden vaikutuksia ja toivutaan niistä ilman aiheetonta viivytystä.

Menettelyohjeiden on määriteltävä

- miten tietoturvan hallinta organisoidaan
- millä toimijoilla on vastuu tietoturvasta
- miten vastuuhenkilöt ovat tavoitettavissa.

Ohjeistus on dokumentoitava ja sitä on ylläpidettävä.

2.5.1 Menettelyohjeiden merkitys

Ohjeiden tärkein tavoite on luoda valmiudet selvittää tietoturvaongelman aiheuttaja mahdollisimman nopeasti ja minimoida tapahtuman vaikutukset. Ohjeilla on myös käytännön merkitystä esimerkiksi uutta henkilöstöä koulutettaessa.

Ohjeistuksessa tulee ottaa huomioon myös mahdolliset erityisohjeet merkittävien häiriötilanteiden korjaustoimenpiteistä. Tällaisia erityisohjeita voivat olla esimerkiksi päivystysjärjestelyt tai varallaolojärjestelyt.

Tyypillisesti tietoturvan hallinnan organisointi kuvataan yrityksen sisäisessä tietoturvapolitiikassa, joka on yrityksen johdon hyväksymä tietoturvallisuuden toteuttamista ja tavoitetilaa kuvaava asiakirjakokonaisuus.

2.6 Muutosten hallinta

Verkkotunnusvälittäjän on järjestettävä muutokset, huollot ja päivitykset siten, että ne aiheuttavat mahdollisimman vähän häiriötä välitystoimintaan.

Verkkotunnusvälittäjän on toteutettava verkko-, ohjelmisto-, laitteisto-, konfiguraatio-, rajapinta- ja laitetilamuutokset hallitusti ja suunnitelmallisesti. Muutoksista on aiheuduttava mahdollisimman vähän häiriötä verkkotunnusten välitystoiminnalle.

2.6.1 Muutostöiden suunnittelu

Muutos-, huolto- ja päivitystoimenpiteiden toteuttamista varten on varattava riittävästi aikaa, jotta suunniteltu toimenpide voidaan tehdä hallitusti. Verkkotunnusvälittäjän on määriteltävä ja dokumentoitava muutoksia ohjaavat prosessit ja käytännöt.

Muutoksista aiheutuvat häiriöt, kuten käyttökatkokset, on minimoitava. Koska katkokset voivat kuitenkin olla välttämättömiä, ja suunnitellut muutokset pitäisi pystyä tekemään mahdollisimman virheettömästi, katkosten mitoittamisessa on huomioitava palvelutarpeiden lisäksi myös muutostyön huolellisen toteuttamisen vaatima realistinen ajantarve.

Muutostilanteiden hallitsemiseksi ja haittojen minimoimiseksi verkkotunnusvälittäjän on huolellisesti etukäteen

- suunniteltava muutostyön eteneminen
- laskettava tarvittavat resurssit
- arvioitava muutostyön vaikutukset ja kesto
- suunniteltava jatkotoimenpiteensä, mikäli muutostyö ei onnistu suunnitellusti.

Esimerkiksi laitteiden ohjelmistoja vaihdettaessa tai niiden määrityksiin muutoksia tehtäessä on hyvä mahdollisuuksien mukaan simuloida ohjelmistomuutoksen vaikutuksia etukäteen, jotta esimerkiksi virheet voitaisiin paikantaa ja korjata ennakolta.

2.6.2 Muutostöiden dokumentointi

Verkkotunnusvälittäjän on ennalta määriteltävä ja dokumentoitava muutostöihin liittyvät työt ohjaavat prosessinsa ja käytäntönsä, jotta kaikissa muutostöissä noudatetaan suunnitelmallisuutta ja ennakoitavuutta.

Kutakin muutos-, huolto- tai päivitystoimenpidettä varten verkkotunnusvälittäjän on myös tapauskohtaisesti, määrittelemiensä prosessien ja käytäntöjen mukaisesti, arvioitava ja varattava muutos-, huolto- tai päivitystyön loppuunsaattamiseksi riittävä aika.

2.7 Välitystoiminnan tietosuoja

2.7.1 Fi-verkkotunnusvälittäjä henkilötietojen rekisterinpitäjänä

Fi-verkkotunnusvälittäjät keräävät ja käsittelevät fi-verkkotunnusten käyttäjien henkilötietoja fi-verkkotunnusten rekisteröimiseksi. Välittäjät merkitsevät tiedot Liikenne- ja viestintävirasto Traficom (Traficom) fi-verkkotunnusrekisteriin ja ylläpitävät tietoja mm. tunnuksen käyttäjän yhteystietoja päivittäessään.

Henkilötietojen käsittelystä säädetään EU:n yleisessä tietosuoja-asetuksessa (679/2016) ja tietosuojalaissa (1050/2018). Välittäjät sitoutuvat noudattamaan EU:n tietosuoja-asetuksessa, tietosuojalaissa, sähköisen viestinnän palveluista annetussa laissa (917/2014) ja verkkotunnusmääräyksessä (68/2016 M) välittäjälle säädetyt velvoitteita ilmoittautuessaan Traficomille fi-verkkotunnusvälittäjäksi. Verkkotunnusmääräyksen perustelut ja soveltaminen -dokumentti tarkentaa konkreettisemmin, miten verkkotunnusmääräystä tulee soveltaa käytännössä.

Laki sähköisen viestinnän palveluista sekä verkkotunnusmääräys 68 ovat välittäjän EU:n yleisen tietosuoja-asetuksen mukainen oikeudellinen peruste käsitellä fi-verkkotunnusten käyttäjien henkilötietoja fi-verkkotunnusten rekisteröimiseksi ja hallinnoimiseksi eli välitystoiminnan harjoittamiseksi.

Fi-verkkotunnusvälittäjät tallettavat tiedot fi-verkkotunnusrekisteriin sähköisen viestinnän palveluista annetun lain 164 §:n 2 momentin, 165 §:n, 167 §:n, 168 §:n ja 170 §:n mukaisesti.

Fi-verkkotunnusvälittäjä toimii tietosuoja-asetuksen mukaisena itsenäisenä rekisterinpitäjänä niiden fi-verkkotunnusten käyttäjien henkilötietojen osalta, joita käsittelee välitystoiminnassaan. Näin ollen, fi-verkkotunnusvälittäjä on rekisterinpitäjänä vastuussa fi-verkkotunnusten käyttäjien eli rekisteröityjen henkilötietojen käsittelystä EU:n yleisen tietosuoja-asetuksen velvoitteiden mukaisesti.

Fi-verkkotunnusvälittäjän on itsenäisenä rekisterinpitäjänä pystyttävä osoittamaan noudattavansa tietosuojalainsäädäntöä. Fi-verkkotunnusvälittäjä on velvollinen laatimaan ja julkaisemaan selosteen siitä, kuinka välittäjä käsittelee fi-verkkotunnusten käyttäjien henkilötietoja.

Fi-verkkotunnusvälittäjän on annettava fi-verkkotunnuksen käyttäjälle kaikki henkilötietojen käsittelyä koskevat tiedot tiiviissä, läpinäkyvässä, helposti ymmärrettävässä ja selkeässä muodossa. Fi-verkkotunnusten käyttäjille on kerrottava muun muassa kuka rekisterinpitäjä on, mitä tarkoitusta varten rekisteröidyn henkilötietoja tarvitaan, kuinka kauan henkilötietoja tarvitaan, luovutetaanko henkilötietoja eteenpäin tai siirretäänkö niitä ETA-maiden ulkopuolelle, miten fi-verkkotunnuksen

käyttäjä voi käyttää henkilötietoihin liittyviä oikeuksiaan ja rekisteröidyn oikeuksiin ja vapauksiin kohdistuvista riskeistä.

Fi-verkkotunnusvälittäjän on itsenäisenä rekisterinpitäjänä toteutettava myös asianmukaiset toimenpiteet fi-verkkotunnusten käyttäjien eli rekisteröityjen tietosuojaoikeuksien toteuttamiseksi. Välittäjän on myös helpotettava rekisteröidyn oikeuksien käyttämistä.

Fi-verkkotunnusvälittäjän on arvioitava yleisesti fi-verkkotunnusten käyttäjien henkilötietojen käsittelyn aiheuttamat riskit ja toimenpiteet ja nimettävä tietosuojavastaava. Fi-verkkotunnusvälittäjän on käsiteltävä henkilötietojen tietoturvaloukkaukset ja ilmoitettava niistä tietosuojavaltuutetulle ja tapauksesta riippuen rekisteröidyille EU:n yleisen tietosuoja-asetuksen mukaisesti.

Huom! EU/ETA-alueen ulkopuolella sijaitsevat fi-verkkotunnusvälittäjät eivät voi rekisteröidä fi-verkkotunnuksia yksityishenkilöille. Rajaus koskee niitä välittäjiä, joiden sijaintivaltiolla ei ole EU:n kanssa erikseen solmittua voimassa olevaa tiedonsiirtojärjestelyä. Rajaus koskee myös niitä Yhdysvalloissa sijaitsevia välittäjiä, jotka eivät ole erikseen sertifioituneet noudattamaan tietosuojajärjestelyä.

Fi-verkkotunnusvälittäjän tulee huolehtia asianmukaisista ja riittävästä tiedonsiirtomekanismeista, jos se siirtää henkilötietoja ETA-alueen ulkopuolelle.

Mikäli fi-verkkotunnusvälittäjä käyttää toiminnassaan jälleenmyyjiä tai muita palveluntarjoajia, sen on merkittävä jälleenmyyjää koskevat tiedot fi-verkkotunnusrekisteriin ja pidettävä ne ajantasaisina. Jälleenmyyjät toimivat henkilötietojen käsittelijöinä välittäjän puolesta ja lukuun. Välittäjä vastaa siitä, että sen jälleenmyyjät sitoutuvat ja vastaavat EU:n yleisen tietosuoja-asetuksen artiklan 28 mukaisista käsittelijän velvollisuuksista henkilötietojen käsittelijöinä. Fi-verkkotunnusvälittäjän tulee tehdä jälleenmyyjänsä kanssa asianmukaiset sopimukset ja antaa jälleenmyyjille yksityiskohtaiset ohjeet henkilötietojen käsittelystä. Välittäjä vastaa täysimääräisesti alihankkijoidensa, käyttämiensä muiden palveluntarjoajien tai jälleenmyyjien, veloitteiden suorittamisesta Traficomiin nähden.

Traficom in lakisääteisenä tehtävänä on hallinnoida fi-maatunnusta ja ylläpitää fi-verkkotunnusrekisteriä. Traficom toimii itsenäisenä rekisterinpitäjänä koko fi-verkkotunnusrekisterin tietosisällön osalta ja vastaa fi-verkkotunnusrekisterin tietovarantokokonaisuudesta.

Tietosuojavaltuutetun toimisto on kansallinen valvontaviranomainen, joka valvoo tietosuojalainsäädännön noudattamista Suomessa (tietosuoja.fi).

2.7.2 Fi-verkkotunnusrekisteriin ilmoitettavat henkilötiedot ja välitystoiminnassa käsiteltävät henkilötiedot

Välittäjän tulee lain perusteella ilmoittaa fi-verkkotunnuksen käyttäjästä fi-verkkotunnusrekisteriin seuraavat henkilötiedot, joiden ajantasaisina pitäminen on välittäjän vastuulla:

- Nimi
- Henkilötunnus / muu yksilöivä tunnus
- Postiosoite
- Puhelinnumero
- Yhteyshenkilö ja yhteyshenkilön puhelinnumero (oikeushenkilöiltä)
- Sähköpostiosoite (prosessiosoite)

Myös yhteisöille rekisteröityjen verkkotunnusten rekisteriin ilmoitettavat käyttäjätiedot voivat sisältää henkilötietoja.

2.7.3 Henkilötietojen käsittelyn tarkoitus ja kesto

Fi-verkkotunnusten välittäminen on toimintaa, jolla tarkoitetaan fi-verkkotunnusten rekisteröintimerkintöjen tekemistä fi-verkkotunnusrekisteriin ja näiden tietojen hallinnointia, kuten päivittämistä. Merkintöjä fi-verkkotunnusrekisteriin voi tehdä vain verkkotunnusvälitysilmoituksen Traficomille tehnyt toiminnan harjoittaja eli fi-verkkotunnusvälittäjä.

Fi-verkkotunnus on merkittävä käyttäjän nimiin ja verkkotunnusvälittäjän on merkittävä fi-verkkotunnusrekisteriin verkkotunnuksen käyttäjää koskevat oikeat, ajantasaiset ja yksilöivät tiedot sekä kuulemisiin ja tiedoksiantoihin käytettävä sähköpostiosoite.

Välittäjän velvollisuutena on pitää tiedot oikeina ja ajan tasalla.

Verkkotunnusvälitystoimintaan kuuluvat kaikki ne toimenpiteet, joita verkkotunnusvälittäjä tekee ylläpitääkseen verkkotunnusrekisteriin merkityn verkkotunnuksen tietoja. Hallinnointia on mm. verkkotunnuksen yhteystietojen päivittäminen, verkkotunnuksen voimassaolon uusiminen, verkkotunnuksen siirtäminen käyttäjältä toiselle ja verkkotunnusvälittäjän vaihtaminen.

Välitystoimintaan kuuluu myös ilmoitus- ja neuvontavelvollisuuden hoitaminen.

Mikäli verkkotunnusvälittäjä liittyy verkkotunnukselle nimipalvelimet, on välittäjä vastuussa siitä, että nimipalvelimet toimivat verkkotunnusmääräyksen mukaisesti.

Verkkotunnuksen hallinnointi tarkoittaa myös kykyä merkitä tietoja verkkotunnusrekisteriin Traficomien määrittelemällä teknisellä järjestelyllä sekä kykyä huolehtia toimintansa tietoturvasta.

Mikäli välittäjä tarjoaa fi-verkkotunnuksen käyttäjälle muita kuin fi-verkkotunnusvälitystoiminnalle lain perustella säädettyjä palveluita (esim. kotisivu- tai sähköpostipalveluita, palvelintilaa, tms.) ja välittäjät käsittelevät fi-verkkotunnuksen käyttäjän henkilötietoja muiden palvelujen tarjoamista varten, on välittäjällä oltava henkilötietojen käsittelylle jokin muu EU:n tietosuojasäätöjen mukainen käsittelyperuste.

Fi-verkkotunnusvälittäjä saa käsitellä fi-verkkotunnusrekisteriin merkitsemiään ja rekisterissä ylläpitämiään henkilötietoja vain sen ajan, kun fi-verkkotunnus on kyseisen välittäjän ylläpidossa ja/tai verkkotunnus on voimassa suoja-aikoinen. Fi-verkkotunnusvälittäjä on vastuussa siitä, että se poistaa fi-verkkotunnusten käyttäjien henkilötiedot omista järjestelmistään sen jälkeen, kun tietojen käsittelyperuste eli tunnuksen välitystoiminta päättyy.

2.7.4 Verkkotunnuksen käyttäjän oikeudet

Fi-verkkotunnusvälittäjä on vastuussa siitä, että fi-verkkotunnuksen käyttäjän EU:n yleisen tietosuojasäätöjen mukaiset oikeudet toteutuvat.

Fi-verkkotunnuksen käyttäjän oikeutena on:

1. tietää, mitkä tahot käyttävät hänen henkilötietojaan

Fi-verkkotunnuksen käyttäjän henkilötietoja käsittelee fi-verkkotunnusvälittäjät ja Traficom.

Verkkotunnusvälittäjät saattavat käyttää toiminnassaan alihankkijoita (jälleenmyyjiä), joiden toiminnasta välittäjät vastaavat itse täysimääräisesti.

2. tietää, mihin tarkoitukseen hänen tietojensa käytetään

Fi-verkkotunnuksen käyttäjän henkilötietoja käytetään verkkotunnuksen rekisteröimiseen ja ylläpitoon sekä fi-verkkotunnusriitojen ratkaisuun.

Fi-verkkotunnusvälittäjät rekisteröivät ja ylläpitävät verkkotunnuksia. Traficom ylläpitää fi-verkkotunnusrekisteriä ja ratkaisee fi-verkkotunnusriidat oikeudenhaltijoiden vaatimuksesta.

3. saada pääsy omiin tietoihin

Fi-verkkotunnusvälittäjän ja Traficomin tulee antaa fi-verkkotunnuksen käyttäjälle vahvistus siitä, että häntä koskevia henkilötietoja käsitellään tai niitä ei käsitellä. Jos tietoja käsitellään, fi-verkkotunnuksen käyttäjällä on oikeus saada pääsy omiin tietoihinsa.

4. tarkastaa ja oikaista virheelliset tietonsa

Fi-verkkotunnuksen käyttäjällä on oikeus tehdä omien tietojen tarkastuspyyntö sekä fi-verkkotunnusvälittäjälle että Liikenne- ja

viestintävirastolle. Fi-verkkotunnusvälittäjän tulee oikaista fi-verkkotunnuksen käyttäjää koskevat epätarkat ja virheelliset henkilötiedot.

5. rajoittaa henkilötietojen käsittelyä

Fi-verkkotunnuksen käyttäjä voi osoittaa pyynnön fi-verkkotunnusvälittäjälle ja Traficomille henkilötietojensa käsittelyn rajoittamiseksi yleisen tietosuoja-asetuksen 18 artiklan mukaisissa tilanteissa.

6. tehdä valitus valvontaviranomaiselle

Fi-verkkotunnuksen käyttäjällä on oikeus saattaa asia tietosuojavaltuutetun käsiteltäväksi katsoessaan, että häntä koskevien henkilötietojen käsittelyssä rikotaan sitä koskevaa lainsäädäntöä. Oikeus ei rajoita muita hallinnollisia muutoksenhakukeinoja tai oikeussuojakeinoja.

2.8 Ilmoitusvelvollisuus tietoturvahäiriöistä

Verkkotunnusvälittäjän on ilmoitettava välitystoimintaan kohdistuvista tietoturvahäiriöistä ja -loukkauksista.

Välittäjän on ilmoitettava viipymättä Liikenne- ja viestintävirastolle, jos sen verkkotunnusten välitystoimintaan kohdistuu

- merkittävä tietoturvaloukkaus
- uhka merkittävästä tietoturvaloukkauksesta tai tapahtumasta, joka estää tai häiritsee toimintaa olennaisesti.

Samalla on myös ilmoitettava häiriön tai sen uhan

- arvioitu kesto
- vaikutukset
- korjaustoimenpiteet
- toimenpiteet, joilla häiriön toistuminen pyritään estämään.

Liikenne- ja viestintävirastolle annettavassa merkittävää tietoturvahäiriötä koskevassa ilmoituksessa tulee mahdollisuuksien mukaan selvittää häiriön tai uhan syy ja kuvata, miten häiriö on aiheutunut.

2.8.1 Tietoturvahäiriöstä on ilmoitettava välittömästi

Häiriöilmoitus on tehtävä 24 tunnin kuluessa siitä, kun häiriötilanne on tullut välittäjän tietoon.

Esimerkiksi tilanteessa, jossa verkkotunnusvälittäjän järjestelmään on tunkeuduttu, on välttämätöntä, että valvova viranomainen saa asiasta viipymättä tiedon. Vaarana on, että tunkeutuja voi päästä vapaasti muuttamaan kyseisen välittäjän hallinnoimien verkkotunnusten tietoja, kuten esimerkiksi nimipalvelimia. Uhka voi koskea laajaakin asiakasmäärää riippuen välittäjän asiakaskunnasta.

Ilmoitus tehdään ensisijaisesti sähköpostitse osoitteeseen cert@ficora.fi. Jos tietoturvan häiriötilanne on vakava tai verkkotunnusvälittäjä tarvitsee apua luvattomasti tehtyjen muutosten selvittämiseksi, yhteydenotto on syytä tehdä myös soittamalla välittäjille ilmoitettuun puhelinnumeroon.

Jos kaikkia ilmoituksessa esitettyjä tietoja ei ole saatavilla ja tilannetta on tutkittava tarkemmin, tehdään viimeistään 24 tunnin kuluessa ns. alustava ilmoitus, jota täydennetään mahdollisimman pian, viimeistään kuitenkin kolmen (3) päivän kuluttua alustavasta ilmoituksesta.

Jos tutkimuksista huolimatta verkkotunnusvälittäjä ei pysty antamaan kaikkia tietoja kolmen päivän kuluessa alustavasta ilmoituksesta, on ilmoitettava kyseisessä määräajassa käyttöön saadut tiedot ja perusteltava, miksi loput tiedot ilmoitetaan määräajan jälkeen.

2.8.2 Merkittävät tietoturvaloukkaukset

Merkittävistä välittäjätoimintaan kohdistuvista tietoturvaloukkauksista on ilmoitettava Liikenne- ja viestintävirastolle.

Tietoturvaloukkausten vaikutukset voivat kohdistua tietojen tai tietojärjestelmien luottamuksellisuuteen, eheyteen tai saatavuuteen.

Luottamuksellisuus: Tiedot ja käyttäjätunnuksiin liittyvät todentamistiedot ovat vain niihin oikeutettujen tahojen tiedossa.

Eheys: Tietoja ei ole mahdollista muuttaa oikeudettomasti. Sivullisten ei ole mahdollista vaikuttaa tietojärjestelmien toimintaan.

Saatavuus: Palvelu ja sen sisältämät tiedot ovat siihen oikeutettujen tahojen saatavissa.

Tietoturvaloukkausten merkittävyyden arviointi

Tietoturvaloukkauksen tai muun tapahtuman merkittävyyttä arvioitaessa on kiinnitettävä huomiota tapauksen haitallisiin vaikutuksiin tai tietoturvan vakavuuteen. Merkittävänä voidaan pitää aina sitä, että tietoturvahäiriö kohdistuu johonkin seuraavista suojattavista kohteista:

- verkkotunnusvälittäjän omiin palveluihin ja palvelujen tuotantoon käytettäviin tieto- ja viestintäjärjestelmiin
- verkkotunnusvälittäjän asiakkaiden tietoturvaan, henkilötietojen suojaan tai yrityssalaisuuksien suojaan
- Liikenne- ja viestintäviraston hallinnoimaan Suomen fi-juureen (joko suoraan tai välillisesti verkkotunnusvälittäjään kohdistuneen tietoturvaloukkauksen seurauksena).

Merkittävänä voidaan myös pitää usein toistuvaa, poikkeuksellisen pitkäkestoista tai tahallista vaikuttavaa toimintaa, jolla on negatiivisia vaikutuksia verkkotunnusvälittäjän kykyyn huolehtia välitystoimintansa

tietoturvasta. Lisäksi merkittävänä voidaan pitää sitä, että häiriötä ei ole mahdollista poistaa pelkillä verkkotunnusvälittäjän omilla toimenpiteillä.

Ilmoitusvelvollisuuteen kuuluvia tietoturvaloukkaustyyppejä

Alla oleva luettelo ilmoitettavista tietoturvaloukkaustyypeistä ei ole tyhjentävä, vaan sen on tarkoitus kuvata ilmoituskynnyksen vakavuustasoa. Harkinnan mukaan myös vähäisemmistä tietoturvaloukkauksista ja niiden uhkista kannattaa ilmoittaa Liikenne- ja viestintävirastolle.

Liikenne- ja viestintävirastolle ilmoitettavia merkittäviä tietoturvahäiriöitä ovat esimerkiksi:

- tietomurrot verkkotunnusvälittäjän tietojärjestelmiin
- oikeudeton pääsy verkkotunnusvälittäjän järjestelmään
- verkkotunnusvälittäjän järjestelmässä oleva tietoturvaa vaarantava haavoittuvuus tai konfiguraatiovirhe.
- sisäänkirjautumistunnusten päätyminen kolmannen osapuolen tietoon
- Liikenne- ja viestintäviraston järjestelmiin käytettävien sisäänkirjautumistunnusten päätyminen ulkopuolisille.

Oikeudettomat muutokset

- mahdollisuus oikeudettomasti muuttaa verkkotunnusvälittäjän hallinnoimien verkkotunnusten tietoja
- verkkotunnusvälittäjän oman henkilöstön oikeudettomasti suorittamat muutokset Liikenne- ja viestintäviraston verkkotunnusrekisteriin
- oikeudeton pääsy verkkotunnusvälittäjän asiakkailleen tarjoamaan itsepalveluportaaliin, jonka avulla asiakkaat voivat itse ylläpitää verkkotunnustensa tietoja.

Palvelunestohyökkäykset

- jos verkkotunnusvälittäjän järjestelmä lamaantuu ja/tai asiakkaiden pääsy järjestelmään estyy tai
- järjestelmän häiriö vaikuttaa Liikenne- ja viestintäviraston järjestelmän toimintaan.

Suositus vapaaehtoisista ilmoituksista

Liikenne- ja viestintävirasto suosittelee, että verkkotunnusvälittäjät ilmoittavat harkintansa mukaan Liikenne- ja viestintävirastolle myös merkittävää vähäisemmistä tietoturvaloukkauksista ja niiden uhkista. Näillä tiedoilla voi olla merkitystä Liikenne- ja viestintäviraston muiden tietoturvatehtävien hoitamisen kannalta.

Liikenne- ja viestintävirastolla on oikeus ryhtyä välttämättömiin toimiin fi-verkkotunnuksia hyödyntämällä toteutettavien yleisiin viestintäverkkoihin tai -palveluihin taikka niiden käyttäjiin kohdistuvien merkittävien

tietoturvaloukkausten havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi. Liikenne- ja viestintävirasto voi ryhtyä näihin toimiin verkkotunnuksen käyttäjää kuulematta.

Liikenne- ja viestintäviraston suorittamat välttämättömät toimet voidaan kohdistaa fi-juuren nimipalvelintietoihin ja ne voivat käsittää:

- verkkotunnukseen suuntautuvan liikenteen estämisen tai rajoittamisen
- verkkotunnukseen suuntautuvan liikenteen ohjaamisen toiseen verkko-osoitteeseen
- muut näihin rinnastettavat tekniset toimenpiteet.

Liikenne- ja viestintäviraston erityisinä tehtävinä ovat lisäksi:

- sähköisen viestinnän toimivuuden, häiriöttömyyden ja turvallisuuden edistäminen
- tiedon kerääminen verkko-, viestintä- ja lisäarvopalveluihin kohdistuvista tietoturvaloukkauksista ja niiden uhkista sekä viestintäverkkojen ja -palvelujen vika- ja häiriötilanteista
- tietoturva-asioista sekä viestintäverkkojen ja viestintäpalvelujen toimivuudesta tiedottaminen
- verkko-, viestintä- ja lisäarvopalveluihin kohdistuvien tietoturvaloukkausten ja niiden uhkien selvittäminen.

2.9 Nimipalvelimet

Verkkotunnusvälittäjä vastaa siitä, että asiakkaille tarjottuihin fi-verkkotunnuksiin liitetyt nimipalvelut on määritelty teknisten vaatimusten mukaisesti.

Fi-verkkotunnuksen voi rekisteröidä joko toimivilla nimipalvelimilla tai kokonaan ilman nimipalvelimia. Jos nimipalvelimet kuitenkin annetaan, niiden kaikkien on toimittava. Jos verkkotunnuksen käyttäjä haluaa myöhemmin pitää verkkotunnuksen nimissään siten, ettei siihen ole liitetty mitään toiminnallisuuksia (ns. parkkipalvelu) kuten sähköpostia tai verkkosivuja, on nimipalvelimet poistettava fi-juuresta.

Vaatimukset nimipalvelimille

Verkkotunnus on määriteltävä Liikenne- ja viestintäviraston määräyksen 68/2014 M mukaisesti vähintään kahdelle ja enintään kymmenelle toisistaan riippumattomalle nimipalvelimelle. Tällä varmistetaan verkkotunnuksen toimivuus yhden nimipalvelimen vikaantuessa.

Nimipalvelimet ovat toisistaan riippumattomia silloin, kun nimipalvelimet toimivat

- eri palvelinlaitteilla
- eri IP-osoitteissa
- eri internetyhteyksien takana.

Lisäksi kaikkien nimipalvelimien on oltava

- yhteydessä internet-tietoverkkoon
- tarkastettavissa määritysten osalta Liikenne- ja viestintäviraston suorittamilla nimipalvelukyselyillä.

Liikenne- ja viestintävirasto tarkastaa kaikkien nimipalvelimien toimivuuden säännöllisesti. Jos yksi tai useampi nimipalvelin ei toimi tai nimipalvelinmääritykset ovat virheelliset, Liikenne- ja viestintävirasto lähettää sähköpostitse huomautusviestin verkkotunnusvälittäjälle tai tämän ilmoittamaan nimipalvelimien ylläpitäjän sähköpostiosoitteeseen.

Määrittelyt voi tarkastaa Liikenne- ja viestintäviraston verkkosivuilta löytyvällä nimipalvelintestillä.

Nimipalvelimiin liittyvät tietoturvasuositukset

Liikenne- ja viestintävirasto suositaa, että verkkotunnusten tietojen (AXFR, DNS zone transfer protocol) siirto estetään ulkopuolisilta. Nimipalvelinten ei myöskään tulisi palauttaa oikeaa tietoa kysyttäessä palvelimen ohjelmistoversiota. Oikean ohjelmistoversion palauttaminen saattaa vaarantaa tietoturvan, jos käytetyssä nimipalvelinohjelmiston versiossa on tiedossa oleva tietoturvaongelma.

2.9.1 Nimipalvelinmääritykset

Nimipalvelinten on täytettävä niille asetetut vaatimukset. Suositeltavaa on myös noudattaa standardimuotoisia SOA-tietueiden sarjanumeroita ja ajastimia.

Nimipalvelimissa on oltava NS-tietueet (Name Server), joissa on määritelty kaikki verkkotunnuksen nimipalvelimet. NS-tietueiden on osoitettava palvelimiin, joille on määritelty joko A- tai AAAA-tietueella (tai molemmilla) IP-osoite nimipalvelussa. NS-tietueet voivat olla vain nimipalvelimia, joille verkkotunnus todellisuudessa on määritelty. NS-tietueiden tulee olla yhtenevät fi-juureen määriteltyjen tietojen kanssa.

SOA-tietueen vaatimukset ja suositukset

Verkkotunnuksen nimipalvelimen asetukset määrittelevän SOA-tietueen (Start of Authority) on oltava seuraavien vaatimusten mukainen:

MNAME (Master Name) -kentässä on oltava verkkotunnuksen ensisijaisen nimipalvelimen nimi

RNAME (Responsible Name) -kentässä on oltava toimiva sähköpostiosoite nimipalvelimien ylläpidosta vastaavalle taholle. Sähköpostiosoite on määriteltävä ilman @-merkkiä, joka korvataan pisteellä. Esimerkiksi: hostmaster.domain.fi. Paras käytäntö on määritellä RNAME-kenttään hostmaster-osoite RFC 2142:n mukaisesti.

Liikenne- ja viestintävirasto suosittelee, etteivät SOA-tietueen sarjanumerot ja ajastimet olennaisesti poikkea julkaistuista internet-standardaista ja -suosituksista. Liikenne- ja viestintäviraston suositukset ovat seuraavat:

```
fi.example. 3600 SOA dns.fi.example. hostmaster.fi.example. (  
2018090401 ; serial YYYYMMDDnn  
86400 ; refresh ( 24 hours)  
7200 ; retry ( 2 hours)  
3600000 ; expire (1000 hours)  
172800 ) ; minimum ( 2 days)
```

Sarjanumero

Sarjanumeron suositeltu muoto on YYYYMMDDnn, jossa YYYY tarkoittaa vuotta, MM kuukautta, DD päivää ja nn on juokseva numero, jonka arvon tulee kasvaa jokaisen päivityksen yhteydessä yhdellä. Päivän ensimmäisen version numero on 01. Sarjanumeron avulla voidaan tarkistaa, että kaikilla verkkotunnuksen nimipalvelimilla on samat zone-tietueet. Sarjanumero ei saa olla nolla (0).

Refresh ja retry

Refresh- ja retry-kenttien arvot vaikuttavat siihen, kuinka usein toissijaiset nimipalvelimet tarkistavat, onko verkkotunnuksen nimipalvelintietoja muutettu ensisijaisella nimipalvelimella. Retry-arvo määrittelee ajan, jolloin nimipalvelintietoja yritetään hakea uudelleen, jos edellinen haku on epäonnistunut.

Expire

Expire-kentän arvo ilmaisee, kuinka kauan nimipalvelin säilyttää vanhaa zone-tiedostoa, jos uutta tiedostoa ei ole mahdollista hakea.

TTL

Minimum TTL -kentän arvo (time to live) määrittää oletuselinajan RR-tietueille (resource record). TTL-arvon asettaminen pienemmäksi kuin suositukset on perusteltua tietyissä tapauksissa, kuten nimipalvelinten muutostilanteissa.

2.9.2 Nimipalvelun tietoturvalaajennus DNSSEC

DNSSEC (Domain Name System Security Extensions) on nimipalvelun tietoturvaa parantava palvelu, joka voidaan ottaa käyttöön myös fi-verkkotunnukselle.

DNSSEC on nimipalvelujärjestelmän laajennus, jonka avulla voidaan varmistaa nimipalvelimelta saatavien tietojen luotettavan alkuperä ja eheys.

Kun DNSSEC-tietoturvalaajennus on käytössä fi-verkkotunnuksella, vastaukset nimipalvelukyselyihin allekirjoitetaan sähköisesti. DNSSEC varmistaa, että nimipalvelukyselyihin saadut vastaukset tulevat oikealta lähettäjältä eikä vastaustietoja ole muokattu. Näin kyseiseen verkkotunnuksen liitetyllä verkkosivulla vierailevat voivat varmistua siitä, että heidät ohjataan oikealle verkkosivulle.

Jotta DNSSEC toimisi, on myös käytetyn resolverinimipalvelun tuettava DNSSEC-allekirjoitusten validointia. Muussa tapauksessa DNSSEC-luottamusketjun eheyttä ei voida varmistaa.

Tietoturvalaajennuksen tarjoaminen asiakkaille

Verkkotunnusvälittäjä voi ottaa DNSSEC-palvelun käyttöön allekirjoittamalla verkkotunnuksen tiedot, minkä jälkeen välittäjä voi lisätä verkkotunnukselle DS-tietueet. DS-tietueita voi hallinnoida sekä EPP-rajapinnan että selainkäyttöliittymän kautta. Avainten vaihdon voi automatisoida EPP-rajapinnan avulla.

Sähköisen allekirjoituksen luomiseen tarvitaan

- yksityinen avain, joka on salainen ja ainoastaan omistajan hallussa sekä
- julkinen avain, joka julkaistaan nimipalvelussa omassa tietueessaan.

Allekirjoitus voidaan varmentaa yksityistä avainta vastaavalla julkisella avaimella. Resolverinimipalvelin tekee validoinnin käyttäjän puolesta.

Fi-vyöhykkeen julkiset avaimet julkaistaan juurivyöhykkeessä. Resolverinimipalvelimia ylläpitäville välittäjille suositellaan juurivyöhykkeen luottamusankkurin määrittelemistä nimipalvelimilleen. Luottamusankkuri löytyy IANA:n DNSSEC-sivuilta.

Havainnollistava kuvaus DNSSECin toiminnasta löytyy esimerkiksi Liikenne- ja viestintäviraston DNSSEC-esitteestä. Esite löytyy Liikenne- ja viestintäviraston verkkosivuilta.

Fi-vyöhykkeen DNSSEC-allekirjoittamisessa käytettävät parametrit

- tiivistefunktio: SHA-256
- allekirjoitusalgoritmi: RSA
- NSEC3
- Opt-Out
- Zone Signing Key (ZSK): RSA 1024-bit (lähiaikoina siirrytään 2048-bit avaimen)
- Key Signing Key (KSK): RSA 2048-bit.

KSK-avaimella allekirjoitetaan ainoastaan vyöhykkeen DNSKEY-tietueeryhmä. ZSK-avaimella allekirjoitetaan vyöhykkeen muut nimipalvelutietueet, kuten allekirjoitettujen alivyöhykkeiden DS-tietueet

sekä Fi-vyöhykkeen auktoritatiiviset tietueet. ZSK-avaimen elinikä on yksi kuukausi ja KSK-avaimen elinikä on yksi vuosi.

Lisätiedot:

Lisätietoa DNSSEC-tietoturvalaajennuksesta saa sähköpostiosoitteesta

`fi-domain-tech@ficora.fi`.

2.9.3 Nimipalvelintesti

Liikenne- ja viestintäviraston verkkosivulta löytyvien nimipalvelintestityökalujen avulla voi tarkastaa verkkotunnuksen nimipalveluiden toimivuuden.

Nimipalvelintestillä saa selville

- onko fi-verkkotunnus määritelty nimipalvelimiin Liikenne- ja viestintäviraston vaatimusten mukaisesti
- toimivatko fi-verkkotunnuksen nimipalvelut tällä hetkellä
- onko verkkotunnuksella käytössä DNSSEC-tietoturvapalvelu.

Mikäli Liikenne- ja viestintävirasto on lähettänyt sähköpostitse virheilmoituksen toimimattomista nimipalvelimista, voi nimipalvelintestillä hakea tarkempaa tietoa virheestä.

Voit tarkistaa nimipalvelimien toiminnan myös ennen verkkotunnuksen rekisteröintiä. Mikäli olet tekemässä nimipalvelinmuutosta, voit testata ovatko uudet nimipalvelimet Liikenne- ja viestintäviraston määräysten mukaisia.

2.10 Tekniset rajapinnat

Välittäjä käyttää teknisenä rajapintana fi-verkkotunnusrekisteriin joko selainkäyttöliittymää tai viraston määrittelemää EPP-rajapintaa.

2.10.1 Selainkäyttöliittymä

Verkkotunnusvälittäjä voi kirjautua Liikenne- ja viestintäviraston fi-verkkotunnusrekisteriin selainkäyttöliittymän kautta. Kirjautuminen on kaksivaiheinen.

Kaksivaiheinen tunnistautuminen tarkoittaa, että käyttäjätunnuksen ja salasanan lisäksi tarvitaan kertakirjautumistunnus. Kertakirjautumistunnus on kahdeksannumeroinen kertakäyttöinen salasana, joka toimitetaan välittäjän matkapuhelimeen tekstiviestillä.

Kirjautuminen edellyttää, että välittäjä on ilmoittautunut Liikenne- ja viestintävirastolle.

2.10.2 EPP-rajapinta

EPP (Extensible Provisioning Protocol) on XML-pohjainen tekninen rajapinta, johon verkkotunnusvälittäjä voi kytkeytyä omalla asiakasohjelmallaan.

Liikenne- ja viestintävirasto ei tarjoa valmista asiakasohjelmaa, vaan verkkotunnusvälittäjän on itse ohjelmoitava tai hankittava asiakasohjelma.

EPP-rajapintaa ei ole pakko ottaa käyttöön. Verkkotunnusvälittäjän on myös mahdollista käyttää molempia rajapintoja.

Verkkotunnusvälittäjän asiakasohjelmiston on oltava yhteensopiva Liikenne- ja viestintäviraston EPP-rajapintakuvauksen kanssa. Siinä kuvataan RFC-dokumentteihin perustuvan rajapinnan rajoitukset ja laajennukset tarkemmin.

Ennen kuin verkkotunnusvälittäjä voi ottaa Liikenne- ja viestintäviraston EPP-rajapinnan käyttöönsä, on välittäjän oma asiakasohjelma testattava Liikenne- ja viestintäviraston EPP-testiympäristössä.

EPP-rajapinnan osoite on

`https://epp.domain.fi (portti 700).`

2.10.3 RFC-standardit

Liikenne- ja viestintäviraston EPP-rajapinta perustuu pääasiassa seuraaviin RFC-standardeihin:

- RFC 4310 Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)
- RFC 5730 Extensible Provisioning Protocol (EPP)
- RFC 5731 Extensible Provisioning Protocol (EPP) Domain Name Mapping
- RFC 5732 Extensible Provisioning Protocol (EPP) Host Mapping
- RFC 5733 Extensible Provisioning Protocol (EPP) Contact Mapping
- RFC 5910 Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP).

2.10.4 KATAKRI-vaatimukset käytettäessä EPP-rajapintaa

Katakri on viranomaisten auditointityökalu, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa.

Jos verkkotunnusvälittäjä käyttää teknisenä rajapintana Liikenne- ja viestintäviraston EPP-rajapintaa, verkkotunnusvälittäjän on täytettävä Katakriin kulloinkin voimassa olevan version teknisen tietoturvallisuuden osa-alueen I-osa-alueen mukaiset suojaustason (IV) vaatimuksista johdetut arvioitavat kohdat seuraavilta osin:

3. tietoliikenneturvallisuus

4. tietojärjestelmäturvallisuus.

Katakri-auditointityökaluun on koottu kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset. Katakri itsessään ei aseta tietoturvallisuudelle ehdottomia vaatimuksia, vaan siihen kootut vaatimukset perustuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvallisuusvelvoitteisiin. Katakriassa esitettyjen vaatimusten yhteyteen on merkitty lähdeviittaus läpinäkyvyyden varmistamiseksi.

Vaatimusten osa-alueet

Katakriin kirjatut vaatimukset on jaettu kolmeen osa-alueeseen:

- Turvallisuusjohtamista koskevassa (T) osa-alueessa pyritään varmistamaan siitä, että organisaatiolla on riittävät turvallisuusjohtamisen valmiudet sekä kyvykkyys.
- Fyysistä turvallisuutta koskevassa (F) osa-alueessa kuvataan salassa pidettävien tietojen fyysistä käyttöympäristöä koskevat turvallisuusvaatimukset.
- Teknistä tietoturvallisuutta koskevassa (I) osa-alueessa kuvataan puolestaan tekniselle tietojenkäsittely-ympäristölle asetetut turvallisuusvaatimukset. Tämä osa-alue jakautuu kolmeen käsiteltävän tiedon mukaiseen suojaustasoon (ST IV, ST III, ST II).

Liikenne- ja viestintäviraston EPP-rajapintaa käyttävien verkkotunnusvälittäjien edellytetään täyttävän teknisen tietoturvallisuuden osa-alueen vaatimukset tietoliikenneturvallisuuden ja tietojärjestelmäturvallisuuden osalta.

Vaatimukset koskevat verkkotunnusten välitystoimintaa. Välittäjä vastaa edellä mainittujen vaatimusten täyttymisestä. Tarvittaessa Liikenne- ja viestintävirasto voi auditoida verkkotunnusvälittäjän toiminnan.

Mikäli verkkotunnusten välitystoimintaa harjoittava taho harjoittaa myös muuta toimintaa, vaatimukset eivät koske muita toimintoja.

Liikenne- ja viestintäviraston määräyksessä viitataan kulloinkin voimassa olevaan kriteeristöön. Katakriin voimassa oleva versio on löydettävissä puolustusministeriön verkkosivuilta.

Jos verkkotunnusvälittäjä käyttää teknisenä rajapintana Liikenne- ja viestintäviraston EPP-rajapintaa, on välittäjän täytettävä Katakriin (tietoturvallisuuden auditointityökalu) kulloinkin voimassa olevan version teknisen tietoturvallisuuden osa-alueen I mukaiset suojaustason (IV) vaatimuksista johdetut arvioitavat kohdat seuraavilta osin:

3. tietoliikenneturvallisuus

4. tietojärjestelmäturvallisuus.

2.10.5 EPP-testiympäristö

EPP-rajapintaa käyttävällä välittäjällä on oltava oma asiakasohjelmisto, joka on yhteensopiva Liikenne- ja viestintäviraston EPP-rajapinnan kanssa. Välittäjän asiakasohjelmiston on läpäistävä Liikenne- ja viestintäviraston edellyttämät testit.

Mikäli verkkotunnusvälittäjä käyttää Liikenne- ja viestintäviraston EPP-rajapintaa, on verkkotunnusvälittäjän asiakasohjelmiston vastattava Liikenne- ja viestintäviraston EPP-rajapintakuvausta.

Ennen kuin verkkotunnusvälittäjä voi ottaa Liikenne- ja viestintäviraston EPP-rajapinnan käyttöönsä, tulee välittäjän asiakasohjelmisto testata Liikenne- ja viestintäviraston EPP-testiympäristössä.

Testauksen avuksi Liikenne- ja viestintäviraston sivuilta löytyvät seuraavat dokumentit:

- EPP-testausohje
- EPP-rajapintakuvaus
- XML-skeemat

Testaukseen liittyvät yhteydenotot pyydetään ensisijaisesti sähköpostitse osoitteeseen fi-domain-tech@ficora.fi.

2.10.6 Fi-verkkotunnusten whois-palvelu

Verkkotunnusvälittäjä voi käyttää Liikenne- ja viestintäviraston whois-palvelua, jotta välittäjän asiakkaat saavat selvitettyä, onko tietty fi-verkkotunnus vapaa.

Fi-verkkotunnusten whois-palvelu löytyy osoitteesta whois.fi. Palvelun käyttöön tarvitaan whois-asiakasohjelma, joka löytyy useimmista Unix- ja Linux-käyttöjärjestelmistä.

2.10.7 Domain Availability Service (DAS)

Liikenne- ja viestintäviraston DAS (Domain Availability Service) -palvelu on rakennettu nopeita fi-verkkotunnusten saatavuuskyselyitä varten. Palvelu palauttaa vastauksena sen, onko verkkotunnus vapaana rekisteröitäväksi. Palvelu ei palauta mitään tietoja verkkotunnusten käyttäjästä eikä tarkempia verkkotunnusten tilatietoja.

Palvelu toimii osoitteessa

`das.domain.fi` (portti 715/UDP)

DAS-palvelusta on julkaistu erillinen palvelukuvaus, joka löytyy Liikenne- ja viestintäviraston verkkosivuilta.

2.10.8 OData

Verkkotunnusjärjestelmän OData-rajapinnan kautta on mahdollista saada tietoa organisaatioiden ja yhteisöjen rekisteröimistä verkkotunnuksista (Domains). Lisätietoina aineistossa on myös verkkotunnusten nimipalvelutiedot (NameServers) sekä verkkotunnusten hallinnoijien yhteystiedot.

Huomioi, että rajapinnan kautta ei pääsääntöisesti tarjota tietoa yksityishenkilöiden varaamista verkkotunnuksista. Siksi rajapintaa ei voi käyttää jonkin verkkotunnuksen saatavuuden tarkistamiseen. Muissakin hauissa tämä rajoitus on syytä huomioida. Käytännössä aineisto kattaa noin 80 % verkkotunnuksista.

OData-palvelun tarjoamat tiedot päivitetään kerran vuorokaudessa.

ODATA-palvelusta on julkaistu erillinen palvelukuvaus, joka löytyy välittäjän selainkäyttöliittymästä.

2.11 Välittäjäksi ilmoittautuminen

Fi-verkkotunnusvälittäjäksi aikovan on ennen Liikenne- ja viestintävirastolle ilmoittautumista tutustuttava huolellisesti kaikkiin laissa säädettyihin vaatimuksiin.

Fi-verkkotunnusvälitystoimintaa säätelevät sähköisen viestinnän palveluista annetun lain säädökset. Välittäjäksi aikovan on ensisijaisen tärkeää kartoittaa etukäteen edellytyksensä täyttää kaikki välittäjälle asetetut tietoturva- ja muut velvollisuudet.

Välittäjäksi ilmoittautuminen tapahtuu Liikenne- ja viestintäviraston sähköisellä lomakkeella. Muutoksista verkkotunnusvälittäjän ilmoittamiin tietoihin on viipymättä ilmoitettava Liikenne- ja viestintävirastolle. Virasto suosittelee, että välittäjä päivittäisi tapahtuneet muutokset Liikenne- ja viestintäviraston verkkotunnusrekisteriin kolmen päivän kuluessa.

Välittäjä voi käyttää fi-verkkotunnusten välitystoiminnassa fi-välittäjälogoa. Logon julkaisukelpoiset versiot löytyvät Liikenne- ja viestintäviraston verkkosivuilta.

2.11.1 Lakisääteinen prosessiosoite ja muut sähköpostiosoitteet

Liikenne- ja viestintävirasto käyttää kaikkiin fi-verkkotunnuksiin liittyviin kuulemisiin ja tiedoksiantoihin verkkotunnusrekisteriin merkittyä sähköpostiosoitetta, jolloin verkkotunnuksiin liittyvä asiakirja tai päätös voidaan aina antaa tiedoksi sähköpostilla. Tämän ns. prosessiosoitteen oikeudellinen merkitys on huomattava ja sen ilmoittaminen Liikenne- ja viestintävirastolle on pakollista.

Prosessiosoitteen käyttö mahdollistaa Liikenne- ja viestintäviraston velvoittavien päätösten nopean tiedoksiannon, sillä päätös tai muu asiakirja katsotaan annetun tiedoksi kolmantena päivänä viestin lähettämisestä.

Verkkotunnusvälittäjää koskevan prosessiosoitteen oikeellisuus on merkittävä tieto, jonka ajantasaisuus on erittäin tärkeää välittäjän oman oikeusturvan kannalta. Välittäjän vastuulla on ilmoittaa myös verkkotunnuksen käyttäjän prosessiosoite ja pitää se ajantasaisena.

Liikenne- ja viestintäviraston sähköiseen järjestelmään voi ilmoittaa muitakin sähköpostiosoitteita, jos verkkotunnusvälittäjä pitää tarpeellisena esimerkiksi erottaa verkkotunnusta koskevien päivittäisten tekniluonteisten asioiden käsittelyyn käytettävät sähköpostiosoitteet pakollisesta prosessiosoitteesta.

2.11.2 Jälleenmyyjien välitystoiminta

Liikenne- ja viestintävirasto valvoo verkkotunnusvälittäjien toimintaa. Mikäli verkkotunnusvälittäjä käyttää fi-verkkotunnusten välitystoiminnassa jälleenmyyjä, on välittäjä vastuussa myös näiden toiminnasta. Jälleenmyyjä voi olla esimerkiksi taho, joka hoitaa fi-verkkotunnusten asiakaspalvelun ja laskuttaa asiakkaita. Mikäli välittäjä lisää jälleenmyyjän tiedot fi-verkkotunnusrekisteriin, ne näkyvät fi-verkkotunnusten julkisten whois-tietojen kohdassa Jälleenmyyjä.

Sähköisen viestinnän palveluista annetun lain säädökset velvoittavat nimenomaan välittäjäksi Liikenne- ja viestintävirastolle ilmoittautunutta tahoja. Välittäjän omalla vastuulla on velvoittaa myös jälleenmyyjänsä noudattamaan fi-verkkotunnustoiminnalle asetettuja vaatimuksia.